

Failure Modes, Effects and Diagnostic Analysis

Project:
644 4-20mA / HART Temperature Transmitter
With Option Code QT

Company:
Rosemount Inc.
(Emerson Automation Solutions)
Shakopee, MN
USA

Contract Number: Q24/07-050
Report No.: ROS 11/02-058 R001
Version V3, Revision R5, May 15, 2025
Valerie Motto

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.
© All rights reserved.

Management Summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the 644 4-20mA / HART Temperature Transmitter, (Option Code QT) hardware revision 1 and software revisions 1.1.1 and 1.1.2. A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification per IEC 61508 of a device. From the FMEDA, failure rates are determined. The FMEDA that is described in this report concerns only the hardware of the 644 Temperature Transmitter. For full functional safety certification purposes, all requirements of IEC 61508 must be considered.

The 644 Temperature Transmitter is a two wire, 4 – 20 mA smart device. For safety instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable. This analysis includes the optional T1 transient protector. The transmitter can be equipped with or without display.

Table 1 gives an overview of the different versions that were considered in the FMEDA of the 644 Temperature Transmitter.

Table 1 Version Overview

Option 1	644 Temperature Transmitter (T/C Configuration)
Option 2	644 Temperature Transmitter (RTD Configuration)

The 644 Temperature Transmitter is classified as a Type B[1] element according to IEC 61508, having a hardware fault tolerance of 0.

The failure rate data used for this analysis meet the *exida* criteria for Route 2_H (see Section 5.3) (and the diagnostic coverage resulting from the analysis exceeds the required 60% threshold). Therefore, the 644 Temperature Transmitter meets the hardware architectural constraints for up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) when the listed failure rates are used.

Based on the assumptions listed in 4.3, the failure rates for the 644 Temperature Transmitter are listed in section 4.5.

These failure rates are valid for the useful lifetime of the product, see section 4.7.

The failure rates listed in this report are based on over 400-billion-unit operating hours of industry field failure data. The failure rate predictions reflect realistic failures and include site specific failures due to random human events for average operating conditions, Site Safety Index (SSI) = 2 [N9], [N10].

A user of the 644 Temperature Transmitter can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL).

[1] Type B element: “Complex” element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2, ed2, 2010.

Table of Contents

1 Purpose and Scope 5

2 Project Management 6

2.1 *exida* 6

2.2 Roles of the parties involved 6

2.3 Standards and literature used 6

2.4 Reference documents 7

2.4.1 Documentation provided by Rosemount Inc. 7

2.4.2 Documentation generated by *exida* 8

3 Product Description 9

4 Failure Modes, Effects, and Diagnostic Analysis 10

4.1 Failure categories description 10

4.2 Methodology – FMEDA, failure rates 11

4.2.1 FMEDA 11

4.2.2 Failure rates 11

4.3 Assumptions 12

4.4 Behavior of the Safety Logic Solver 12

4.5 Failure Rate Results 13

4.6 Proof Test Coverage 14

4.6.1 Partial Proof Test 1 15

4.6.2 Comprehensive Proof Test 2 15

4.6.3 Comprehensive Proof Test 3 16

4.6.4 Proof Test Coverage Summary 16

4.7 Useful Life 17

4.8 Architecture Constraints 17

5 Using the FMEDA Results 18

5.1 Temperature sensing devices 18

5.1.1 644 Temperature Transmitter with thermocouple 18

5.1.2 644 Temperature Transmitter with RTD 19

5.2 PFD_{avg} calculation 644 Temperature Transmitter 20

5.3 *exida* Route 2_H Criteria 21

6 Terms and Definitions 22

7 Status of the Document 23

7.1 Liability 23

7.2 Version History 23

7.3 Future enhancements 24

7.4 Release signatures 24

Appendix A Failure rates for various transmitter modes 25
Appendix B *exida* Environmental Profiles 28
Appendix C Determining Safety Integrity Level 29
Appendix D Site Safety Index 33
D.1 Site Safety Index Profiles 33

1 Purpose and Scope

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the 644 Temperature Transmitter. From this, failure rates for each failure mode/category, useful life, and proof test coverage are determined.

The information in this report can be used to evaluate whether an element meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and if applicable, the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511.

A FMEDA is part of the effort needed to achieve full certification per IEC 61508 or other relevant functional safety standard.

2 Project Management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety, availability, and cybersecurity with over 500 person years of cumulative experience in functional safety, alarm management, and cybersecurity. Founded by several of the world's top reliability and safety experts from manufacturers, operators and assessment organizations, *exida* is a global corporation with offices around the world. *exida* offers training, coaching, project-oriented consulting services, safety engineering tools, detailed product assurance, ANSI National Accreditation Board (ANAB) accredited functional safety and cybersecurity certification and Irish National Accreditation Board (INAB) accredited machinery safety certification. *exida* maintains a comprehensive failure rate and failure mode database on electronic and mechanical components and a comprehensive database on solutions to meet safety standards such as IEC 61508.

2.2 Roles of the parties involved

Rosemount Inc.	Manufacturer of the 644 Temperature Transmitter
Exida	Performed the hardware assessment

Rosemount Inc. contracted *exida* in November 2011 with the hardware assessment of the above-mentioned device.

2.3 Standards and literature used

The services delivered by *exida* were performed based on the following standards / literature.

[N1]	IEC 61508-2: ed2, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical Component Reliability Handbook, 4th Edition, 2017	*exida* LLC, Electrical Component Reliability Handbook, Fourth Edition, 2017
[N3]	Mechanical Component Reliability Handbook, 4th Edition, 2017	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, Fourth Edition, 2017
[N4]	Goble, W.M. 2010	Control Systems Safety Evaluation and Reliability, 3rd edition, ISA, ISBN 97B-1-934394-80-9. Reference on FMEDA methods
[N5]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition

[N6]	O'Brien, C., Gavin, R., & Bredemeyer, L., 2023	*exida* LLC., Final Elements in Safety Instrumented Systems, IEC61511 Compliant Systems and IEC 61508 Compliant Products, Second Edition, 2023, ISBN 978-1-934977-24-8
[N7]	Scaling the Three Barriers, Recorded Web Seminar, June 2013	Scaling the Three Barriers, Recorded Web Seminar, June 2013, http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers
[N8]	Meeting Architecture Constraints in SIF Design, Recorded Web Seminar, March 2013	http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design
[N9]	Random versus Systematic – Issues and Solutions, September 2016	Goble, W.M., Bukowski, J.V., and Stewart, L.L., Random versus Systematic – Issues and Solutions, exida White Paper, PA: Sellersville, www.exida.com/resources/whitepapers, September 2016.
[N10]	Assessing Safety Culture via the Site Safety Index™, April 2016	Bukowski, J.V. and Chastain-Knight, D., Assessing Safety Culture via the Site Safety Index™, Proceedings of the AIChE 12th Global Congress on Process Safety, GCPS2016, TX: Houston, April 2016.
[N11]	Quantifying the Impacts of Human Factors on Functional Safety, April 2016	Bukowski, J.V. and Stewart, L.L., Quantifying the Impacts of Human Factors on Functional Safety, Proceedings of the 12th Global Congress on Process Safety, AIChE 2016 Spring Meeting, NY: New York, April 2016.
[N12]	Criteria for the Application of IEC 61508:2010 Route 2H, December 2016	Criteria for the Application of IEC 61508:2010 Route 2H | exida
[N13]	Using a Failure Modes, Effects and Diagnostic Analysis (FMEDA) to Measure Diagnostic Coverage in Programmable Electronic Systems, November 1999	Goble, W.M. and Brombacher, A.C., Using a Failure Modes, Effects and Diagnostic Analysis (FMEDA) to Measure Diagnostic Coverage in Programmable Electronic Systems, Reliability Engineering and System Safety, Vol. 66, No. 2, November 1999.
[N14]	FMEDA – Accurate Product Failure Metrics, June 2015	Grebe, J. and Goble W.M., FMEDA – Accurate Product Failure Metrics, www.exida.com, June 2015.

2.4 Reference documents

2.4.1 Documentation provided by Rosemount Inc.

[D1]	00644-7401, Rev AB, 10/13/11	Terminal Cap Assembly 644
[D2]	00644-7100, Rev AC, 5 Mar 2012	Schematic, 644 Electronics Board Headmount
[D3]	00644-7110, Rev 01, 5/3//11	Schematic, 644 Hart and Fieldbus Transient Protector, T1

		Option
[D4]	Fault Injection List 644T_27Mar2012_results.xls , 28 Mar 2012	644 Fault Injection Test Results
[D5]	Fault_Injection_Test_Details.doc, 28 Mar 2012	644 Fault Injection Test Result Details
[D6]	644 Next Generation Transmitter Safety Integrity Requirements Specification Revision: A.4, 2 Nov 2011	644 Safety Integrity Requirements Specification
[D7]	644NG Diagnostic Design.doc	644 Diagnostics Design, attached to 27 Oct 2011 e-mail from Corey Wolf (Rosemount)
[D8]	00644-7600, Rev AB, 11 Oct 2011	Temperature Transmitter Hub Assembly 644, includes hardware revision history
[D9]	644_vdd.htm	software release notes/version description document, shows released software drawing number
[D10]	00644-7300, Rev AA, 9 Apr 2012	644 HART Software Revision Drawing, associates software release drawing (dash #) with NE-53 software revision

2.4.2 Documentation generated by *exida*

[R1]	644NG TT and sensing devices Rev AB.xls	Failure rate calculations Summary, 644 Temperature Transmitter, August 2012
[R2]	644NG Temp Transmitter part 1 of 3 Rev AB.xls	Failure rate calculations, 644 Temperature Transmitter, April 2012
[R3]	644NG Temp Transmitter part 2 of 3 Rev AB.xls	Failure rate calculations, 644 Temperature Transmitter, April 2012
[R4]	644NG Temp Transmitter Common Portion of part 3 of 3 Rev AB.xls	Failure rate calculations Common Portion, 644 Temperature Transmitter, April 2012
[R5]	644NG Temp Transmitter TC Portion of Rev AB.xls	Failure rate calculations T/C Portion, 644 Temperature Transmitter, April 2012
[R6]	644NG Temp Transmitter Dual TC Portion of Rev AB.xls	Failure rate calculations Dual T/C, 644 Temperature Transmitter, April 2012
[R7]	644NG Temp Transmitter 3 Wire RTD Portion of Rev AB.xls	Failure rate calculations 3 Wire RTD, 644 Temperature Transmitter, April 2012
[R8]	644NG Temp Transmitter Dual 3 Wire RTD Portion of Rev AB.xls	Failure rate calculations Dual 3 Wire RTD, 644 Temperature Transmitter, April 2012
[R9]	CombinedPTCoverage2 - 3144_644 - 2025-05-13.xlsx	PT Coverage for 3144 provided by Micro Motion, exida updated failure rates and added 644 calculations

3 Product Description

The 644 Temperature Transmitter is a two wire, 4 – 20 mA smart device. For safety instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable. The transmitter can be equipped with or without display.

Combined with one or two temperature sensing elements, the 644 transmitter becomes a temperature sensor assembly. The temperature sensing elements that can be connected to the 644 Temperature Transmitter are:

- 2-, 3-, and 4-wire RTD
- Thermocouple
- Millivolt input (–10 to 100mV)
- 2-, 3-, and 4-wire Ohm input (0 to 2000Ω)

The FMEDA has been performed for different input sensing element configurations of the 644 transmitter, i.e., 3-wire RTD, 4-wire RTD, and thermocouple. Estimates have been made of the temperature sensing element failure rates given the ability of the 644 transmitter to detect several failure modes of the temperature sensing element.

644 HART SIS Capabilities and Options

- Single or Dual sensor inputs for RTD, Thermocouple, mV and Ohm
- DIN A Head mount and Field mount transmitters
- SIL3 Capable: IEC 61508 certified by an accredited 3rd party agency for use in safety instrumented systems up to SIL 3 [Minimum requirement of single use (1oo1) for SIL 2 and redundant use (1oo2) for SIL 3]
- LCD display
- Enhanced display with Local Operator Interface
- Integral Transient Protection
- Diagnostic Suite
- Enhanced accuracy and stability
- Transmitter-Sensor Matching with Callendar Van Dusen constants

The 644 Temperature Transmitter is classified as a Type B[2] element according to IEC 61508, having a hardware fault tolerance of 0.

[2] Type B element: “Complex” element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2, ed2, 2010.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation in section 2.4.1 and is documented in [R1] to [R9].

4.1 Failure categories description

In order to judge the failure behavior of the 644 Temperature Transmitter, the following definitions for the failure of the device were considered.

Fail-Safe State	State where the process reaches a safe situation. Depending on the application the fail-safe state is defined as the output going to fail low or fail high.
Fail Safe	Failure that causes the device to go to the defined fail-safe state without a demand from the process.
Fail Detected	Failure that causes the output signal to go to the predefined alarm state. (These failures may be converted to the selected fail-safe state.)
Fail Dangerous	Failure that deviates the process signal or the actual output by more than 2% of span, drifts away from the user defined threshold (Trip Point) and that leaves the output within the active scale.
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by automatic diagnostics.
Fail Dangerous Detected	Failure that is dangerous but is detected by automatic diagnostics.
Fail High	Failure that causes the output signal to go to the maximum output current (> 20.9 mA, output saturate high) or high alarm (>21 mA)
Fail Low	Failure that causes the output signal to go to the minimum output current (< 3.7 mA, output saturate low) or low alarm (3.5, 3.75 mA).
No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function.
Annunciation Detected	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is detected by internal diagnostics. A Fail Annunciation Detected failure leads to a false diagnostic alarm.
Annunciation Undetected	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is not detected by internal diagnostics.

The failure categories listed above expand on the categories listed in IEC 61508 in order to provide a complete set of data needed for design optimization.

Depending on the application, a Fail High or a Fail Low failure can either be safe or dangerous and may be detected or undetected depending on the programming of the logic solver. Consequently, during a Safety Integrity Level (SIL) verification assessment the Fail High and Fail Low failure categories need to be classified as safe or dangerous, detected or undetected.

The Annunciation failures are provided for those who wish to do reliability modeling more detailed than required by IEC61508. It is assumed that the probability model will correctly account for the Annunciation failures.

4.2 Methodology – FMEDA, failure rates

4.2.1 FMEDA

A FMEDA (Failure Mode Effect and Diagnostic Analysis) is a failure rate prediction technique based on a study of design strength versus operational profile stress. It combines design FMEA techniques with extensions to identify automatic diagnostic techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each failure mode category [N13, N14].

4.2.2 Failure rates

The accuracy of any FMEDA analysis depends upon the component reliability data as input to the process. Component data from consumer, transportation, military or telephone applications could generate failure rate data unsuitable for the process industries. The component data used by *exida* in this FMEDA is from the Electrical and Mechanical Component Reliability Handbooks [N2] [N3] which were derived using failure data formulas based upon:

- Over 400 billion unit operational hours of industry field failure data from multiple sources.
- Technical reports such as IEC 62380, SN 29500 and industry sources.
- Manufacturer Meetings.
- Component Research

The *exida* profile chosen for this FMEDA was 2 as this was judged to be the best fit for the product and application information submitted by Rosemount Inc..

Early life failures (infant mortality) are not included in the failure rate prediction as it is assumed that commission testing is done. End of life failures are not included in the failure rate prediction as useful life is specified.

The failure rates are predicted for a Site Safety Index of SSI=2 [N10], [N11] as this level of operation is common in many industries. Failure rate predictions for other SSI levels are included in the exSILentia® tool from *exida*.

The user of these numbers is responsible for determining the failure rate applicability to any particular environment. *exida* Environmental Profiles listing expected stress levels can be found in Appendix D. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant. exida has detailed models available to make customized failure rate predictions. Contact *exida* for assistance.

Accurate plant specific data may be used to check validity of this failure rate data. If a user has data collected from a good proof test reporting system such as *exida* SILStat™ that indicates higher failure rates, the higher numbers shall be used.

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the 644 Temperature Transmitter.

- The worst-case assumption of a series system is made. Therefore, only a single component failure will fail the entire 644 Temperature Transmitter.
- Failure rates are constant for the useful life period.
- Any product component that cannot influence the safety function (feedback immune) is excluded. All components that are part of the safety function including those needed for normal operation are included in the analysis.
- The stress levels are specified in the *exida* Profile used for the analysis are limited by the manufacturer's published ratings.
- Practical fault insertion tests have been used when applicable to demonstrate the correctness of the FMEDA results.
- The HART protocol is only used for setup, calibration, and diagnostics purposes, not for safety critical operation.
- The application program in the logic solver is constructed in such a way that Fail High and Fail Low failures are detected regardless of the effect, safe or dangerous, on the safety function.
- Materials are compatible with process conditions.
- The device is installed and operated per manufacturer's instructions.
- External power supply failure rates are not included.
- Worst-case internal fault detection time is <1 hour.

4.4 Behavior of the Safety Logic Solver

Depending on the application, the following scenarios are possible:

- Low Trip: the safety function will go to the predefined fail-safe state when the process value below a predefined low set value. A current < 3.75mA (Fail Low) is below the specified trip-point.
- High Trip: the safety function will go to the predefined fail-safe state when the process value exceeds a predefined high set value. A current > 21mA (Fail High) is above the specified trip-point.

The Fail Low and Fail High failures can either be detected or undetected by a connected logic solver. The PLC Detection Behavior in Table 2 represents the under-range and over-range detection capability of the connected logic solver.

Table 2 Application example

Application	PLC Detection Behavior	λ_{low}	λ_{high}
Low trip	< 4mA	= λ_{sd}	= λ_{du}
Low trip	> 20mA	= λ_{su}	= λ_{dd}
Low trip	< 4mA and > 20mA	= λ_{sd}	= λ_{dd}
Low trip	-	= λ_{su}	= λ_{du}
High trip	< 4mA	= λ_{dd}	= λ_{su}
High trip	> 20mA	= λ_{du}	= λ_{sd}
High trip	< 4mA and > 20mA	= λ_{dd}	= λ_{sd}
High trip	-	= λ_{du}	= λ_{su}

In this analysis it is assumed that the logic solver is able to detect under-range and over-range currents, therefore the yellow highlighted behavior is assumed.

4.5 Failure Rate Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the 644 Temperature Transmitter FMEDA.

Table 3 and Table 4 list the failure rates for the 644 Temperature Transmitter with a Site Safety Index (SSI) of 2 (good site maintenance practices). See Appendix F for an explanation of SSI and the failure rates for SSI of 4 (ideal maintenance practices).

Table 3 Failure rates 644 Temperature Transmitter (T/C configuration)

Failure category		Failure rate (in FITs)			
		Single T/C mode		Dual T/C mode	
Fail High (detected by the logic solver)			31		31
Fail Low (detected by the logic solver)			331		340
	Fail detected (int. diag.)[3]	303		312	
	Fail low (inherently)	28		28	
Fail Dangerous Undetected			39		39
No Effect			124		128
Annunciation Undetected			12		12

[3] These failures follow the setting of the Alarm switch and result in either a High or Low output of the transmitter. It is assumed that upon the detection of a failure the output will be sent downscale, therefore all detected failures are listed as a sub-category of the Fail Low failure category. If the Alarm switch is set to High Alarm, these failures would need to be added to the Fail High failure category.

Table 4 Failure rates 644 Temperature Transmitter (RTD configuration)

Failure category		Failure rate (in FITs)			
		Single RTD mode		Dual RTD mode	
Fail High (detected by the logic solver)		31		31	
Fail Low (detected by the logic solver)		286		299	
	Fail detected (int. diag.)[3]	258		271	
	Fail low (inherently)	28		28	
Fail Dangerous Undetected		30		31	
No Effect		119		123	
Annunciation Undetected		12		12	

Table 5 lists the failure rates for the 644 Temperature Transmitter according to IEC 61508.

Table 5 Failure rates with Good Maintenance Assumptions in FIT @ SSI=2 according to IEC 61508

Application/Device/Configuration	λ_{SD}	λ_{SU}[4]	λ_{DD}	λ_{DU}	#	SFF
644 Single T/C mode	0	0	362	39	136	90.3%
644 Dual T/C mode	0	0	371	39	140	90.5%
644 Single RTD mode	0	0	317	30	131	91.4%
644 Dual RTD mode	0	0	330	31	135	91.4%

Where:

λ_{SD} = Fail Safe Detected

λ_{SU} = Fail Safe Undetected

λ_{DD} = Fail Dangerous Detected

λ_{DU} = Fail Dangerous Undetected

= No Effect Failures

These failure rates are valid for the useful lifetime of the product, see Section 4.7.

4.6 Proof Test Coverage

According to section 7.4.5.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by automatic diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the Failure Modes, Effects, and Diagnostic Analysis can be detected during proof testing.

[4] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.

4.6.1 Partial Proof Test 1

Proof test 1 consists of an analog output Loop Test, as described in Table 6. This test will detect approximately 63% of possible DU failures in the transmitter and approximately 90% of the simple sensing element DU failures. This means a Proof Test Coverage of 66% for the overall sensor assembly, assuming a single 4-wire RTD is used.

Table 6 Steps for Proof Test 1

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip
2	Send a HART command to the transmitter to go to the high alarm current output and verify that the analog current reaches that value. This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance. This also tests for other possible failures.
3	Send a HART command to the transmitter to go to the low alarm current output and verify that the analog current reaches that value. This tests for possible quiescent current related failures
4	Use the HART communicator to view detailed device status to ensure no alarms or warnings are present in the transmitter
5	Perform reasonability check on the sensor value(s) versus an independent estimate (i.e. from direct monitoring of BPCS value) to show current reading is good
6	Restore the loop to full operation
7	Remove the bypass from the safety PLC or otherwise restore normal operation

4.6.2 Comprehensive Proof Test 2

The alternative proof test consists of the following steps, as described in Table 7. This test will detect approximately 96% of possible DU failures in the transmitter and approximately 99% of the simple sensing element DU failures. This results in a Proof Test Coverage of 96% for the overall sensor assembly, assuming a single 4-wire RTD is used.

Table 7 Steps for Proof Test 2

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip
2	Perform Proof Test 1
3	Verify the measurement for two temperature points for Sensor 1. Verify the measurement for two temperature points for Sensor 2, if second sensor is present.
4	Perform reasonability check of the housing temperature
5	Restore the loop to full operation
6	Remove the bypass from the safety PLC or otherwise restore normal operation

4.6.3 Comprehensive Proof Test 3

The third proof test consists (as described in Table 8) of a comprehensive transmitter and a limited sensor proof test combination. This test will detect approximately 96% of possible DU failures in the transmitter and approximately 90% of the simple sensing element DU failures. This results in a Proof Test Coverage of 95% for the overall sensor assembly, assuming a single 4-wire RTD is used.

Table 8 Steps for Proof Test 3

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip
2	Perform Proof Test 1
3	Connect calibrated sensor simulator in place of sensor 1
4	Verify safety accuracy of 2 temperature points inputs to transmitter.
5	If sensor 2 is used, repeat steps 3 and 4.
6	Restore sensor connections to transmitter.
7	Perform reasonability check of transmitter housing temperature.
8	Perform reasonability check on the sensor(s) values versus an independent estimate (i.e. from direct monitoring of BPCS value) to show current reading is acceptable.
9	Restore loop to full operation.
10	Remove the bypass from the safety PLC or otherwise restore normal operation

4.6.4 Proof Test Coverage Summary

Table 9 Proof Test Coverage Summary

Device	$\lambda_{DU}PT$ (FIT)	Proof Test Coverage
644 + 4-wire RTD, Partial	33	66%
644 + 4-wire RTD, Comprehensive 1	33	96%
644 + 4-wire RTD, Comprehensive 2	33	95%
644 + 3-wire RTD, Partial	34	67%
644 + 3-wire RTD, Comprehensive 1	34	96%
644 + 3-wire RTD, Comprehensive 2	34	95%
644 + Thermocouple, Partial	46	67%
644 + Thermocouple, Comprehensive 1	46	96%
644 + Thermocouple, Comprehensive 2	46	95%

4.7 Useful Life

The Useful Life of the device predicted by component failure data is 50 years.

4.8 Architecture Constraints

According to IEC 61508-2 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508-2 or the 2_H approach according to 7.4.4.3 of IEC 61508-2, or the approach according to IEC 61511:2016 which is based on 2_H (see Section 5.3).

The 1_H approach involves calculating the Safe Failure Fraction for the entire element.

The 2_H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508.

The failure rate data used for this analysis meet the *exida* criteria for Route 2_H which is more stringent than IEC 6150802 (and the diagnostic coverage resulting from the analysis exceeds the required 60% threshold). Therefore, the 644 Temperature Transmitter meets the hardware architectural constraints for up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) when the listed failure rates are used.

The architectural constraint type for the 644 Temperature Transmitter is B. The hardware fault tolerance of the device is 0.

A user of the 644 Temperature Transmitter can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL.

5 Using the FMEDA Results

The following section(s) describe how to apply the results of the FMEDA.

5.1 Temperature sensing devices

The 644 Temperature Transmitter together with a temperature-sensing device becomes a temperature sensor assembly. Therefore, when using the results of this FMEDA in a SIL verification assessment, the failure rates and failure modes of the temperature sensing device must be considered. Typical failure rates for close-coupled thermocouples and RTDs are listed in Table 10.

Table 10 Typical failure rates close-coupled thermocouples and RTDs

Temperature Sensing Device	Failure rate (FIT)
Thermocouple low stress environment	102
Thermocouple high stress environment	408
3-wire RTD low stress environment	49
3-wire RTD high stress environment	195
4-wire RTD low stress environment	51
4-wire RTD high stress environment	205

The following sections give examples on how to combine the temperature-sensing element failure rates and the transmitter failures. The examples given are for PV (Process Value) set to represent Sensor 1 or Sensor 2 when using a single sensor, either T/C or RTD. More information on how to combine temperature-sensing element failure rates and transmitter failure rates for other configurations, including the use of dual sensing-elements is given in Appendix A.

5.1.1 644 Temperature Transmitter with thermocouple

The failure mode distributions for thermocouples vary in published literature but there is strong agreement that open circuit or “burn-out” failure is the dominant failure mode. While some estimates put this failure mode at 99%+, a more conservative failure rate distribution suitable for SIS applications is shown in Table 11 when close-coupled thermocouples are supplied with the 644 Temperature Transmitter in *exida* Profile 2. The drift failure mode is primarily due to T/C aging. The 644 Temperature Transmitter will detect a thermocouple burnout failure and drive the analog output to the specified failure state.

Table 11 Typical failure mode distributions for thermocouples

TC Failure Modes – Close-coupled device	Percentage
Open Circuit (Burn-out)	93%
Wire Short (Temperature measurement in error)	6%
Drift (Temperature measurement in error) (50% Safe; 50% Dangerous)	1%

A complete temperature sensor assembly consisting of 644 Temperature Transmitter and a closely coupled thermocouple supplied with the 644 Temperature Transmitter can be modeled by considering a series subsystem where failure occurs if there is a failure in either component. For such a system, failure rates are added. Assuming that the 644 Temperature Transmitter is programmed to drive its output to the specified failure state on detected failures of the thermocouple, the failure rate contribution for the thermocouple in a low stress environment is:

λ_{SU}= (102) * (0.005) = 0.5 FIT

λ_{DD} = (102) * (0.93) = 94.9 FIT

λ_{DU} = (102) * (0.06 + 0.005) = 6.6 FIT

The total for the temperature sensor assembly with the 644 Temperature Transmitter is:

λ_{SU} = 0.5 + 0 = 0.5 FIT

λ_{DD} = 94.9 + 362 = 456.9 FIT

λ_{DU} = 6.6 + 39 = 45.6 FIT

These numbers could be used in safety instrumented function SIL verification calculations for this set of assumptions. For these circumstances, the Safe Failure Fraction of this temperature sensor assembly is 90.9%.

5.1.2 644 Temperature Transmitter with RTD

The failure mode distribution for an RTD also depends on the application with key variables being stress level, RTD wire length and RTD type (2/3 wire or 4 wire). The key stress variables are high vibration and frequent temperature cycling as these are known to cause cracks in the substrate leading to broken lead connection welds. Typical failure rate distributions in *exida* Profile 2 are shown in Table 12. The 644 Temperature Transmitter will detect open circuit and short circuit RTD failures and drive its output to the alarm state on detected failures of the RTD.

Table 12 Failure mode distribution for 4-wire RTD, low stress environment

RTD Failure Modes – Close-coupled device	Percentage	
	3-wire RTD	4-wire RTD
Open Circuit	78%	81%
Short Circuit	4%	7%
Drift (Temperature measurement in error) (50% Safe; 50% Dangerous)	18%	12%

A complete temperature sensor assembly consisting of 644 Temperature Transmitter and a closely coupled, cushioned 3-wire RTD supplied with the 644 Temperature Transmitter can be modeled by considering a series subsystem where failure occurs if either component fails. For such a system, failure rates are added. Assuming that the 644 Temperature Transmitter is programmed to drive its output to the alarm state on detected failures of the RTD, the failure rate contribution for a close-coupled 3-wire RTD in a low stress environment is:

λ_{SU} = (49) * (0.09) = 4.4 FIT

λ_{DD} = (49) * (0.78 + 0.04) = 36.3 FIT

λ_{DU} = (49) * (0.09) =4.4 FIT

The total for the temperature sensor assembly with the 644 Temperature Transmitter is:

λ_{SU} = 4.4 + 0 = 4.4 FIT

λ_{DD} = 36.3 + 317 = 353.3 FIT

λ_{DU} = 4.4 + 30 = 34.4 FIT

These numbers could be used in safety instrumented function SIL verification calculations for this set of assumptions. The Safe Failure Fraction for this temperature element, given the assumptions, is 91.2%.

Assuming that the 644 Temperature Transmitter is programmed to drive its output to the alarm state on detected failures of the RTD, the failure rate contribution for a close-coupled 4-wire RTD in a low stress environment is:

λ_{SU} = (51) * (0.06) = 3.1 FIT

λ_{DD} = (51) * (0.81 + 0.07) = 44.9 FIT

λ_{DU} = (51) * (0.06) = 3.1 FIT

The total for the temperature sensor assembly with the 644 Temperature Transmitter is:

λ_{SU} = 3.1 + 0 = 3.1 FIT

λ_{DD} = 44.9 + 317 = 361.19 FIT

λ_{DU} = 3.1 + 30 = 33.1 FIT

These numbers could be used in safety instrumented function SIL verification calculations for this set of assumptions. The Safe Failure Fraction for this temperature element, given the assumptions, is 91.7%.

5.2 PFD_{avg} calculation 644 Temperature Transmitter

Using the failure rate data displayed in section 4.5, and the failure rate data for the associated element devices, an average the Probability of Failure on Demand (PFD_{avg}) calculation can be performed for the element.

Probability of Failure on Demand (PFD_{avg}) calculation uses several parameters, many of which are determined by the particular application and the operational policies of each site. Some parameters are product specific and the responsibility of the manufacturer. Those manufacturer specific parameters are given in this third-party report.

Probability of Failure on Demand (PFD_{avg}) calculation is the responsibility of the owner/operator of a process and is often delegated to the SIF designer. Product manufacturers can only provide a PFD_{avg} by making many assumptions about the application and operational policies of a site. Therefore, use of these numbers requires complete knowledge of the assumptions and a match with the actual application and site.

Probability of Failure on Demand (PFD_{avg}) calculation is best accomplished with *exida's* exSILentia tool. See Appendix E for a complete description of how to determine the Safety Integrity Level for an element. The mission time used for the calculation depends on the PFD_{avg} target and the useful life of the product. The failure rates and the proof test coverage for the element are required to perform the PFD_{avg} calculation. The proof test coverage for the suggested proof test are listed in section 4.6.

5.3 *exida* Route 2_H Criteria

IEC 61508, ed2, 2010 describes the Route 2_H alternative to Route 1_H architectural constraints. The standard states:

> "based on data collected in accordance with published standards (e.g., IEC 60300-3-2: or ISO 14224); and, be evaluated according to
>
> - the amount of field feedback; and
> - the exercise of **expert judgment**; and when needed
> - the undertaking of specific tests,
>
> in order to estimate the average and the uncertainty level (e.g., the 90% confidence interval or the probability distribution) of each reliability parameter (e.g., failure rate) used in the calculations."

exida has interpreted this to mean not just a simple 90% confidence level in the uncertainty analysis, but a high confidence level in the entire data collection process. As IEC 61508, ed2, 2010 does not give detailed criteria for Route 2_H, *exida* has established the following:

1. field unit operational hours of 10,000,000 per each component or known common usage of the component for over ten years in at least 10 units; and
2. operational hours are counted only when the data collection process has been audited for correctness and completeness; and
3. failure definitions are realistic without data censoring of failures with both a systematic and random failure cause [N9]; and
4. every component used in an FMEDA meets the above criteria.

This set of requirements is chosen to assure high integrity failure data suitable for safety integrity verification [N12].

6 Terms and Definitions

Automatic Diagnostics	Tests automatically performed online internally by the device or, if specified, externally by another device without manual intervention or manual interpretation of the results .
DC	Diagnostic Coverage
exida 2H criteria	A method to arriving at failure rates suitable for use in hardware evaluations utilizing the 2_H Route with more detail and more requirements than specified in IEC 61508-2.
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3).
FIT	Failure in Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
PFD_{avg}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction summarizes the fraction of failures which lead to a safe state plus the fraction of failures which will be detected by automatic diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Type A element	“Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
Type B element	“Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

7 Status of the Document

7.1 Liability

exida prepares FMEDA reports based on methods advocated in engineering literature and International technical reports. Failure rates are obtained from field failure studies and other sources. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

Due to future potential changes in the standards, product design changes, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical model number product at some future time.

Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years, contact the product vendor to verify the current validity of the results.

7.2 Version History

Contract Number	Report Number	Revision Notes
Q24/07-050	ROS 11-02-058 R001 V3 R5	Added PT Coverage Summary Table and T/C RTD Calculations at customer request, Updated failure rates for RTD and T/C from latest CRD in Profile 2. Added Option Code QT back to Product Description. This is still required to indicate the safety-certified version. Correction to 644 Single RTD mode # Failure Rate. VAM 13-May-2025
Q23/05-006	ROS 11-02-058 R001 V3 R4	Clarification to SW version (1.1.X and 1.2.X → 1.1.1 and 1.1.2); VAM
Q16/12-041	ROS 11-02-058 R001 V3 R3	Updated error messages; TES
Q16/12-041	ROS 11-02-058 R001 V3 R2	Removed reference per customer request; TES
Q16/12-041	ROS 11-02-058 R001 V3 R1	updated per IEC 61508 2nd ed; updated per template T-001 V11 R2
Q11/02-058	ROS 11-02-058 R001 V2 R2	Updated per customer comments; TES 1/23/15
Q11/02-058	ROS 11-02-058 R001 V2 R1	Updated Proof Test; TES 11/21/14
Q11/02-058	ROS 11-02-058 R001 V1 R2	changed product name on cover sheet, corrected PDFavg graph
Q11/02-058	ROS 11-02-058 R001 V1 R1	updated with comments in 27 April 2012 e-mail, released to Rosemount; 15 May 201
Q11/02-058	ROS 11-02-058 R001 V0 R1	Initial version; 20 April 2012

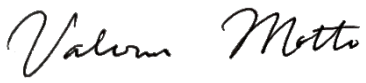
Reviewer: Rudy Chalupa, 15 May 2025

Status: Released, 15 May 2025

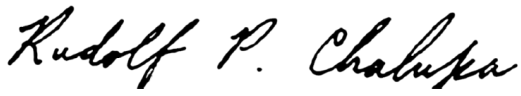
7.3 Future enhancements

At request of client.

7.4 Release signatures



Valerie Motto, CFSP, Senior Safety Engineer



Rudolf P. Chalupa, CFSE, Principal Safety Engineer

Appendix A Failure rates for various transmitter modes

This Appendix discusses in more detail how to combine the 644 Temperature Transmitter failure rates with sensing element failure rates and how to take credit for diagnostics provided by the transmitter on the sensing element (Drift Alert = Alarm).

Table 13 644 Temperature Transmitter modes

S1 Type	S2 Type	Suspend Non-PV Faults	Drift Alert[6]	Primary Variable (PV)	Calculation
T/C, 3 Wire RTD, 4 wire RTD	Disabled	X	N/A	S1	1
Disabled	T/C, 3 Wire RTD	X	N/A	S2	1
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Disable	S1	1
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Alarm	S1	2
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Disable	S1	1
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Alarm	S1	2*
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Disable	S2	1
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Alarm	S2	2
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Disable	S2	1
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Alarm	S2	2
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Disable	Differential	3
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Alarm	Differential	3
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Disable	Differential	3
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Alarm	Differential	3
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Disable	Average	3
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Alarm	Average	4
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Disable	Average	3*
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Alarm	Average	4*
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Disable	First Good	1
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Alarm	First Good	2
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Disable	First Good	1*
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Alarm	First Good	2

* These modes represent “Hot back-up”. Using the calculation method as described will results in accurate numbers for PFD_{AVG}, but will overestimate the false trip rate. (The sensing elements are configured as a 2oo2 voting and will not alarm on a single sensor failure).

Calculation 1

Single Sensor configured, PV = S1 or PV = S2 or,

Dual Sensors configured, PV = S1, PV = S2 or PV = First Good and Drift Alert = disabled

[6] For purposes of safety validation, Drift Alert = Warning is considered the same as Drift Alert = disabled

Modeled as a series subsystem where failure occurs if either sensing element or transmitter fails. For such a system, failure rates are added. Use single mode failure rates for the 644 Temperature Transmitter and add sensing element failure rates (single element). This has been described in detail in sections 5.1.1 and 5.1.2.

Calculation 2

Dual Sensors configured, PV = S1 or PV = S2 or PV = First Good, and Drift Alert = alarm

Modeled as a series subsystem where failure occurs if either component fails. For such a system, failure rates are added. Use dual mode failure rates for the 644 Temperature Transmitter and add sensing element failure rates (single element). The sensing element failure rates should reflect the additional coverage on the drift failures (99%) provided by the Drift Alert.

Example: 644 with dual 3-wire RTDs

Table 14 Typical failure mode distributions for 3-wire RTDs, Low Stress environment / cushioned sensor

RTD Failure Modes – Close coupled element	Percentage
Open Circuit	78%
Short Circuit	4%
Drift (Temperature measurement in error)	18%

Assuming that the 644 Temperature Transmitter is programmed to drive the output low on detected failure, the failure rate contribution for the 3-wire RTD in a low stress environment is:

- λ^{L} = (49) * (0.78 + 0.04 + 0.99·0.18) = 48.9 FITs
- λ^{DU} = (49) * (0.01·0.18) = 0.1 FITs

When these failure rates are added to the failure rate of the 644 Temperature Transmitter, single RTD mode (see Table 4, first Failure rate column), the total for the temperature sensor subsystem is:

- λ^{L} = 48.9 + 286 = 334.9 FITs
- λ^{H} = 31 FITs
- λ^{DU} = 0.1 + 30 = 30.1 FITs

Calculation 3

Dual Sensors configured, PV = Average or PV = Differential mode, Drift Alert = disabled

Both sensing elements need to function. Use single mode failure rates for the 644 Temperature Transmitter (single mode failure rates are selected because Drift Alert = disabled) and add failure rates for both sensing elements.

Example: 644 with dual 3-wire RTDs

Assuming that the 644 Temperature Transmitter is programmed to drive the output low on detected failure, the failure rate contribution for the 3-wire RTD in a low stress environment is:

- λ^{L} = 2 * ((49) * (0.78 + 0.04)) = 80.4 FITs
- λ^{DU} = 2 * ((49) * (0.18)) = 17.6 FITs

When these failure rates are added to the failure rate of the 644 Temperature Transmitter, single RTD mode (see Table 4, first Failure rate column), the total for the temperature sensor subsystem is:

- λ^{L} = 80.4 + 286 = 366.4 FITs
- λ^{H} = 31 FITs
- λ^{DU} = 17.6 + 31 = 48.6 FITs

Calculation 4

Dual Sensors configured, PV = Average and Drift Alert = alarm

To obtain the overall failure rates of the sensor assembly, use the dual mode failure rates for the 644 Temperature Transmitter and add failure rates for both sensing elements. The sensing element failure rates should be adjusted to reflect the additional coverage on the drift failures (99%) provided by the Drift Alert.

Example: 644 with dual 3-wire RTDs

Assuming that the 644 Temperature Transmitter is programmed to drive the output low on detected failure, the failure rate contribution for the 3-wire RTD in a low stress environment is:

- λ^{L} = 2 * ((49 * (0.78 + 0.04 + 0.99·0.18)) = 97.8 FITs
- λ^{DU} = 2 * ((49 * (0.01·0.18)) = 0.2 FITs

When these failure rates are added to the failure rate of the 644 Temperature Transmitter, dual RTD mode (see Table 4, second column), the total for the temperature sensor subsystem is:

- λ^{L} = 97.8 + 299 = 396.8 FITs
- λ^{H} = 31 FITs
- λ^{DU} = 0.2 + 31 = 31.2 FITs

Appendix B *exida* Environmental Profiles

Table 15 *exida* Environmental Profiles

***exida* Profile**	**1**	**2**	**3**	**4**	**5**	**6**
Description (Electrical)	Cabinet mounted/ Climate Controlled	Low Power Field Mounted no self-heating	General Field Mounted self-heating	Subsea	Offshore	N/A
Description (Mechanical)	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
IEC 60654-1 Profile	B2	C3 also applicable for D1	C3 also applicable for D1	N/A	C3 also applicable for D1	N/A
Average Ambient Temperature	30 C	25 C	25 C	5 C	25 C	25 C
Average Internal Temperature	60 C	30 C	45 C	10 C	45 C	Process Fluid Temp.
Daily Temperature Excursion (pk-pk)	5 C	25 C	25 C	2 C	25 C	N/A
Seasonal Temperature Excursion (winter average vs. summer average)	5 C	40 C	40 C	2 C	40 C	N/A
Exposed to Elements / Weather Conditions	No	Yes	Yes	Yes	Yes	Yes
Humidity[7]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[8]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[9]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[10]	G2	G3	G3	G3	G3	Compatible Material
Surge[11]						
Line-Line	0.5 kV	0.5 kV	0.5 kV	0.5 kV	0.5 kV	N/A
Line-Ground	1 kV	1 kV	1 kV	1 kV	1 kV	
EMI Susceptibility[12]						
80 MHz to 1.4 GHz	10 V/m	10 V/m	10 V/m	10 V/m	10 V/m	N/A
1.4 GHz to 2.0 GHz	3 V/m	3 V/m	3 V/m	3 V/m	3 V/m	
2.0Ghz to 2.7 GHz	1 V/m	1 V/m	1 V/m	1 V/m	1 V/m	
ESD (Air)[13]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

[7] Humidity rating per IEC 60068-2-3
[8] Shock rating per IEC 60068-2-27
[9] Vibration rating per IEC 60068-2-6
[10] Chemical Corrosion rating per ISA 71.04
[11] Surge rating per IEC 61000-4-5
[12] EMI Susceptibility rating per IEC 61000-4-3
[13] ESD (Air) rating per IEC 61000-4-2

Appendix C Determining Safety Integrity Level

The information in this appendix is intended to provide the method of determining the Safety Integrity Level (SIL) of a Safety Instrumented Function (SIF). **The numbers used in the examples are not for the product described in this report.**

Three things must be checked when verifying that a given Safety Instrumented Function (SIF) design meets a Safety Integrity Level (SIL) [N4] and [N7].

These are:

A. Systematic Capability or Prior Use Justification for each device meets the SIL level of the SIF;

B. Architecture Constraints (minimum redundancy requirements) are met; and

C. a PFD_{avg} calculation result is within the range of numbers given for the SIL level.

A. Systematic Capability (SC) is defined in IEC61508:2010. The SC rating is a measure of design quality based upon the methods and techniques used to design and development a product. All devices in a SIF must have a SC rating equal or greater than the SIL level of the SIF. For example, a SIF is designed to meet SIL 3 with three pressure transmitters in a 2oo3 voting scheme. The transmitters have an SC2 rating. The design does not meet SIL 3. Alternatively, IEC 61511 allows the end user to perform a "Prior Use" justification. The end user evaluates the equipment to a given SIL level, documents the evaluation and takes responsibility for the justification.

B. Architecture constraints require certain minimum levels of redundancy. Different tables show different levels of redundancy for each SIL level. A table is chosen and redundancy is incorporated into the design [N8].

C. Probability of Failure on Demand (PFD_{avg}) calculation uses several parameters, many of which are determined by the particular application and the operational policies of each site. Some parameters are product specific and the responsibility of the manufacturer. Those manufacturer specific parameters are given in this third-party report.

A Probability of Failure on Demand (PFD_{avg}) calculation must be done based on a number of variables including:

1. Failure rates of each product in the design including failure modes and any diagnostic coverage from automatic diagnostics (an attribute of the product given by this FMEDA report);
2. Redundancy of devices including common cause failures (an attribute of the SIF design);
3. Proof Test Intervals (assignable by end user practices);
4. Mean Time to Restore (an attribute of end user practices);
5. Proof Test Effectiveness; (an attribute of the proof test method used by the end user with an example given by this report);
6. Mission Time (an attribute of end user practices);
7. Proof Testing with process online or shutdown (an attribute of end user practices);
8. Proof Test Duration (an attribute of end user practices); and
9. Operational/Maintenance Capability (an attribute of end user practices).

The product manufacturer is responsible for the first variable. Most manufacturers use the *exida* FMEDA technique which is based on over 400 billion hours of field failure data in the process industries to predict these failure rates as seen in this report. A system designer chooses the second variable. All other variables are the responsibility of the end user site. The exSILentia® SILVer™ software considers all these variables and provides an effective means to calculate PFD_{avg} for any given set of variables.

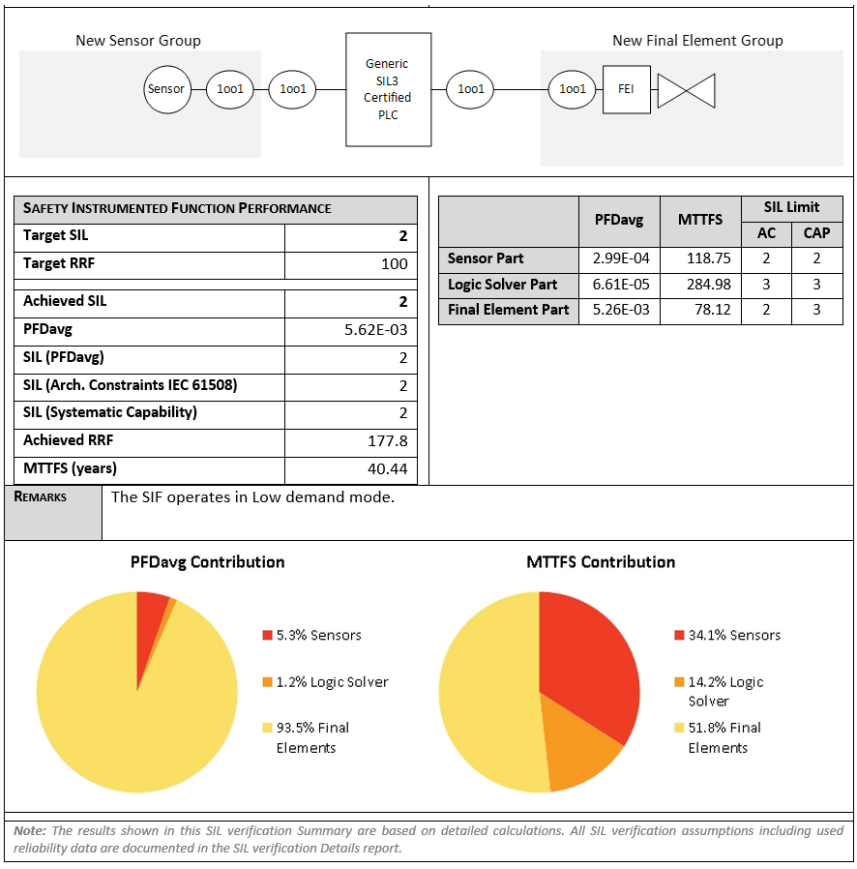
Simplified equations often account for only for the first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic assumptions stated. These assumptions often result in optimistic PFD_{avg} calculations and have indicated SIL levels higher than reality. Therefore, idealistic equations should not be used for actual SIF design verification.

All the variables listed above are important. As an example, consider a high-level protection SIF. The proposed design has a single SIL 3 certified level transmitter, a SIL 3 certified safety logic solver, and a single remote actuated valve consisting of a certified solenoid valve, certified scotch yoke actuator and a certified ball valve. Note that the numbers chosen are only an example and not the product described in this report.

Using exSILentia with the following variables selected to represent results from simplified equations:

- Mission Time = 5 years
- Proof Test Interval = 1 year for the sensor and final element, 5 years for the logic solver
- Proof Test Coverage = 100% (ideal and unrealistic but commonly assumed)
- Proof Test done with process offline

This results in a PFD_{avg} of 5.62E-03 which meets SIL 2 with a risk reduction factor of 179. The subsystem PFD_{avg} contributions are Sensor PFD_{avg} = 2.99E-04, Logic Solver PFD_{avg} = 6.61E-05, and Final Element PFD_{avg} = 5.26E-03. See Figure 1.



Safety Instrumented Function Performance	
Target SIL	2
Target RRF	100
Achieved SIL	2
PFDavg	5.62E-03
SIL (PFDavg)	2
SIL (Arch. Constraints IEC 61508)	2
SIL (Systematic Capability)	2
Achieved RRF	177.8
MTTFS (years)	40.44

	PFDavg	MTTFS	SIL Limit	
			AC	CAP
Sensor Part	2.99E-04	118.75	2	2
Logic Solver Part	6.61E-05	284.98	3	3
Final Element Part	5.26E-03	78.12	2	3

Remarks: The SIF operates in Low demand mode.

Note: The results shown in this SIL verification Summary are based on detailed calculations. All SIL verification assumptions including used reliability data are documented in the SIL verification Details report.

Figure 1: exSILentia results for idealistic variables.

If the Proof Test Interval for the sensor and final element is increased in one year increments, the results are shown in Figure 2.

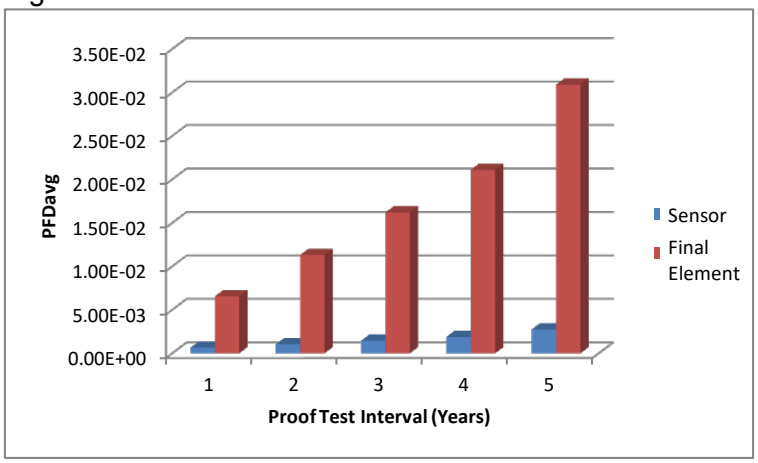


Figure 2 PFD_{avg} versus Proof Test Interval.

If a set of realistic variables for the same SIF are entered into the exSILentia software including:

- Mission Time = 25 years
- Proof Test Interval = 1 year for the sensor and final element, 5 years for the logic solver
- Proof Test Coverage = 90% for the sensor and 70% for the final element
- Proof Test Duration = 2 hours with process online.
- MTTR = 48 hours
- Maintenance Capability = Medium for sensor and final element, Good for logic solver

with all other variables remaining the same, the PFD_{avg} for the SIF equals 3.80E-02 which barely meets SIL 1 with a risk reduction factor 26 The subsystem PFD_{avg} contributions are Sensor PFD_{avg} = 1.13E-03, Logic Solver PFD_{avg} = 1.55E-04, and Final Element PFD_{avg} = 3.68E-02 (Figure 3).

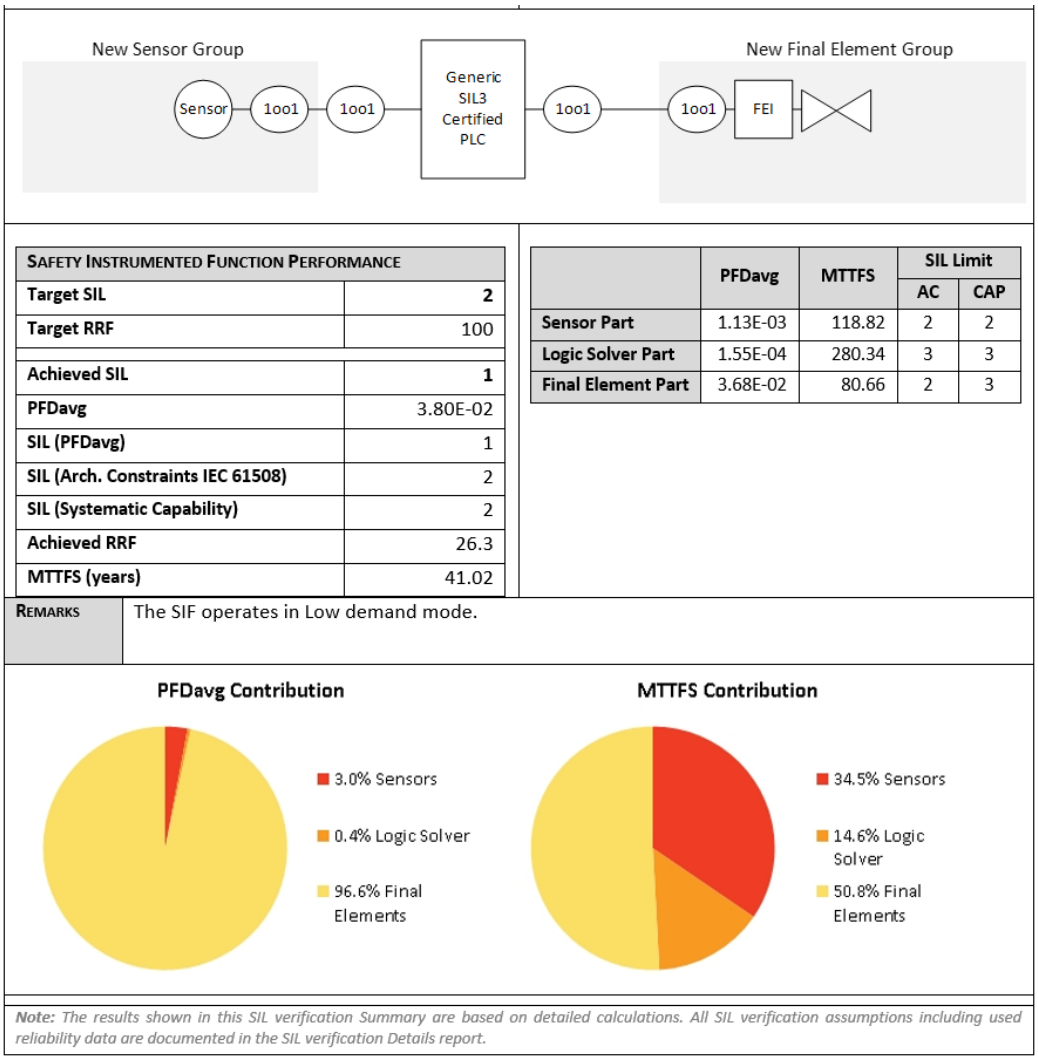


Figure 3: exSILentia results with realistic variables

It is clear that PFD_{avg} results can change an entire SIL level or more when all critical variables are not used.

Appendix D Site Safety Index

Numerous field failure studies have shown that the failure rate for a specific device (same Manufacturer and Model number) will vary from site to site. The Site Safety Index (SSI) was created to account for these failure rates differences as well as other variables. The information in this appendix is intended to provide an overview of the Site Safety Index (SSI) model used by *exida* to compensate for site variables including device failure rates.

D.1 Site Safety Index Profiles

The SSI is a number from 0 – 4 which is an indication of the level of site activities and practices that contribute to the safety performance of SIFs on the site. Table 16 details the interpretation of each SSI level. Note that the levels mirror the levels of SIL assignment and that SSI 4 implies that all requirements of IEC 61508 and IEC 61511 are met at the site and therefore there is no degradation in safety performance due to any end-user activities or practices, i.e., that the product inherent safety performance is achieved.
Several factors have been identified thus far which impact the Site Safety Index (SSI). These include the quality of:
Commission Test
Safety Validation Test
Proof Test Procedures
Proof Test Documentation
Failure Diagnostic and Repair Procedures
Device Useful Life Tracking and Replacement Process
SIS Modification Procedures
SIS Decommissioning Procedures
and others

Table 16 *exida* Site Safety Index Profiles

Level	Description
SSI 4	Perfect - Repairs are always correctly performed, Testing is always done correctly and on schedule, equipment is always replaced before end of useful life, equipment is always selected according to the specified environmental limits and process compatible materials. Electrical power supplies are clean of transients and isolated, pneumatic supplies and hydraulic fluids are always kept clean, etc. Note: This level is generally considered not possible but retained in the model for comparison purposes.
SSI 3	Almost perfect - Repairs are correctly performed, Testing is done correctly and on schedule, equipment is normally selected based on the specified environmental limits and a good analysis of the process chemistry and compatible materials. Electrical power supplies are normally clean of transients and isolated, pneumatic supplies and hydraulic fluids are mostly kept clean, etc. Equipment is replaced before end of useful life, etc.
SSI 2	Good - Repairs are usually correctly performed, Testing is done correctly and mostly on schedule, most equipment is replaced before end of useful life, etc.
SSI 1	Medium – Many repairs are correctly performed, Testing is done and mostly on schedule, some equipment is replaced before end of useful life, etc.
SSI 0	None - Repairs are not always done, Testing is not done, equipment is not replaced until failure, etc.

END OF DOCUMENT